Pivoting

Let's say that you have compromised one machine on a network and you want to keep going to another machine. You will use the first machine as a staging point/plant/foothold to break into machine 2. Thid technique of using one compromised machine to access another is called pivoting. Machine one is the `pivot` in the example. The `pivot` is just used as a way to channel/tunnel our attack.

Ipconfig

We are looking for machines that have at least THREE network interfaces (loopback, eth0, and eth1 (or something)). These machines are connected to other networks, so we can use them to pivot.

```
 # Windows
ipconfig /all
route print

#Linux
ifconfig
ifconfig -a
```

Metasploit

Ping-sweep the network

First we want to scan the network to see what devices we can target. In this example we already have a meterpreter shell on a windows machine with SYSTEM-privileges.

```
meterpreter > run arp_scanner -r 192.168.1.0/24
```

This command will output all the devices on the netowork.

Scan each host

Now that we have a list of all available machines. We want to portscan them.

We will to that portscan through metasploit. Using this module:

```
use auxiliary/scanner/portscan/tcp
```

If we run that module now it will only scan machines in the network we are already on. So first we need to connect us into the second network.

On the already pwn machine we do

```
ipconfig
```

Now we add the second network as a new route in metasploit. First we background our session, and then do this:

```
 # the ip addres and the subnet mask, and then the meterpreter session
route add 192.168.11.1 255.255.255.0 1
```

Now we can run our portsanning module:

```
use auxiliary/scanner/portscan/tcp
```

Attack a specific port

In order to attack a specific port we need to forwards it like this

```
portfwd add -l 3389 -p 3389 -r 192.168.1.222
```

This is a good video-explanation: https://www.youtube.com/watch?v=c0XiaNAkjJA

https://www.offensive-security.com/metasploit-unleashed/pivoting/

http://ways2hack.com/how-to-do-pivoting-attack/